G/A

Argentine

TOP SECRET - 1 - TICOM/I-172

INTERROGATIONS OF HAGEN AND PASCHKE OF PERS ZS.

Attached is a report on the interrogation of Fräulein HAGEN and O.R.R. Adolf PASCHKE of Pers ZS, which was carried out by Commander BULL, R.N.V.R., at Military Government Offices, MARBURG LAHN, on 11th and 13th September, 1945. The report is concerned almost entirely with British Diplomatic systems, together with a short section on South American cyphers.

See also Ticom/I-27.

TICOM

6 December 1945 No. of pages 7

DISTRIBUTION

British

D.D.3
H.C.G.
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
C.C.R.
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (4) (via Lt.Cdr. Manson)
G-2 (via Lt.Col. Hilles)
A.S.A. (4) (via Capt. Collins)
Director, S.I.D. USFET
Col. Kunkel, USAAFE.

TICOM

S.A.C. (3)
Cdr. Bacon
Lt. Cdr. Manson
Major Cowan
Capt. Collins
Ticom Files (4)

Additional

Mr. Kendrick, Berkeley St.

1. British Foreign Office Long Subtractors

(See Ticom/I-22, paragraphs 23, 96 and 141)

Frl. HAGEN stated that British Foreign Office long subtractor traffic had been handled almost entirely by KUNZE and that she had only been given a general summary of his work from time to time. He had worked first from the indicators and had compiled tables of common differences - later this had been done with Hollerith machinery. By this means he had succeeded in stripping some of the recypher after a few months, but there was not sufficient time, material or staff for him to recover the plain language. In any case, the work was not done currently enough to justify any high priority. In 1938, they worked with an average depth of 6 to 8; in 1939 this sometimes rose to a peak of 15, but even so the book was never broken. The messages were addressed to Washington, Cairo, Moscow, Berlin and Helsinki, and included consulates as well as embassies.

2. HAGEN believed that only a few hundred groups of the recyphering table and a "few thousand" relative groups of plain cypher text were recovered; KUNZE had told her that he thought he had enough to attack the book, but just at that time - in 1940-41 - he came to the conclusion that there had been a change of basic book. She stated that only perhaps half a dozen groups were identified for certain, e.g. fullstop. Had there been any real success, she would have been charged with the book-building, as opposed to the mathematical work done by KUNZE. HAGEN did not know how much back traffic had been stripped with the help of Recyphering Table M9 (which KUNZE stated had been captured in Norway). She believed that the basic book was the same as that mentioned above, but thought that she would have heard if there had been any striking success.

2. HAGEN believed that only a few hundred groups of the recyphering table and a "few thousand" relative groups of plain cypher text were recovered; KUNZE had told her that he thought he had enough to attack the book, but just at that time - in 1940-41 - he came to the conclusion that there had been a change of basic book. She stated that only perhaps half a dozen groups were identified for certain, e.g. fullstop. Had there been any real success, she would have been charged with the book-building, as opposed to the mathematical work done by KUNZE. HAGEN did not know how much back traffic had been stripped with the help of Recyphering Table M9 (which KUNZE stated had been captured in Norway). She believed that the basic book was the same as that mentioned above, but thought that she would have heard if there had been any striking success.

3. She said that Inter-Departmental Cypher was the only captured book which Pers ZS had received from the British Consulate at Bergen and that they had no others except a captured Portuguese book which had been handed over by the Italians. She knew nothing of any Italian organisation for "pinching" cyphers. She stated that in 1944-45, they received unparaphrased literal texts of F.O. cypher telegrams from a "secret source" at the British Embassy in Ankara. There were half a dozen which all dealt with Turkish cyphers suggesting that British cyphers should be used. They compared these with cypher intercepts but none could be identified with certainty. These messages were only shown to a few people by SELCHOW, and possibly KUNZE and KRUG had not seen them.

4. HAGEN was then asked about the presented depth provided by telegrams sent as Number 1 on 1st January on the same table. She said that there were sometimes as many as 20 to 23 of these but could give no details of particular years. She was not aware that these had ever extended beyond the first of January.

5. She said that the basic books were thought to have changed at the end of 1941 and that after that date they had very few depths to work on. She thought that several basic books were in force simultaneously besides I.D. but did not know for certain. They had a lot of material on the Berne and Teheran links but would have needed a special staff to make a detailed study of these. She stated that F.O. traffic tended to have stereotyped beginners but could not recall any of the groups in question.

6. They had studied a lot of messages prefixed INTER which were believed to be special traffic on a separate book from diplomatic; also a great number with address "Moveable" which were formerly in letters and later in figures. She remembered prefix CXG then "Moveable" even before the war. They received some messages addressed "Unexpected" but these were not studied.

Classification of Systems

7. HAGEN gave the following information on previously unidentified German classifications:-

B 23 - African G.T.C.

B 24 - A 5-letter code with very little traffic; "something quite unimportant". She did not remember where it came from.

B 26 - A 5-letter code with only a few telegrams; not worked on.

(Although we are only aware of the existence of one South African G.T.C., the Pers ZS documents indicated three, viz. B 23, B 24 and B 26.) HAGEN felt sure that these were all different codes. She said that on B 23 there was quite a lot of traffic at the beginning of the war - two or three telegrams daily to and from South Africa and London with telegraphic address "Oppositely". These dealt with political and economic questions and were quite interesting until 1944, when they changed to uninteresting material such as freight details. There was very little traffic on the others and they were never read. She also remembered the group HUNYD for fullstop from a systematic "Indian Code" in 1939-40; traffic was of little interest and mainly concerned passports, etc.

8. She could not remember any details of B 27 (which appears to have been a South African four-letter code). She said that Dominions Office Confidential Code was not worked on, since there was insufficient traffic. She thought that Colonial Office Confidential Code, known as TNKE, was worked on by the Forschungsamt but later put aside because there was not enough traffic. Indian Word Code (the "Indian Code" mentioned above) was read by the Forschungsamt but was of little interest. Canadian G.T.C. was never read because they only had a few telegrams. No "B" numbers were given to these codes or to recyphered systems.

9. India Office Systems.

They had very little traffic on India Office Cypher "S" and this was not worked on. Code "Q" was broken after about six months with gaps; they intercepted about six telegrams a day. Most of the traffic consisted of news guidance, and sometimes there were reports on Indian speeches, etc. Current Indian newspapers were comparatively difficult to obtain and the Staatssekretär was always interested to read these decodes. No signals of outstanding interest were sent on this system.

10. Foreign Office "R" Codes.

(See Ticom/I-22, paragraphs 92, 94 and 108.)

HAGEN stated that it took about six months to break R Code 1941; 2000 groups had to be identified before the book could be considered effectively broken. The only cribs which they had from the press, B.B.C., etc., were pre-war. Shortly before the war, they read a message on B 25 dealing with general F.O. policy regarding Germany which was of particular interest. Normally there was an interesting message on this code about once a week. Their only captured book was R 1935 (B 25) which was found at Bergen.

11. Eire

HAGEN described the work done by Pers ZS on Irish Diplomatic substitution recoding tables for use with G.T.C. There were 26 hatted alphabets, each group being taken from one alphabet. The alphabets were

not necessarily used in order but always systematically. The last group of a telegram indicated the system to be used in the next message, e.g. if the last group was recyphered with alphabet 5, then this alphabet would also be used for the first group of the next message. The tables changed at irregular intervals - only about four times during the war. Different keys were used for various posts, e.g. Berne, Rome, Berlin, Paris, Madrid. The traffic became more difficult to read in 1942-43, when there was insufficient material and not enough staff. Then the Forschungsamt started work on it and solved the Berlin and Madrid links. Pers ZS took over the keys from the Forschungsamt in 1944. The first three figures of the message gave the page number, the fourth figure the number of the block, and the fifth and sixth figures the line-numbers. This new system used a 300-figure subtractor; each end of the link was allotted 25 such keys, e.g. 25 Dublin-Berlin and 25 Berlin-Dublin, etc. If the length of the message exceeded 300 figures, the key was repeated, but a new key was used for each new message, always in the order 1 to 25.

Messages consisted of reports from the Irish minister on the state of affairs in Germany. The Staatssekretär was interested in diplomatic reports on the trend of events, air-raids, etc. The traffic was regarded as valuable by Ribbentrop and some messages were shown to Hitler. HAGEN said that with any luck six fairly long messages were sufficient to break a new substitution recoding table, and this work took less than a week.

Irish messages in plain G.T.C. did not provide information of any value.

12. Commercial Cyphers.

HAGEN said that Pers ZS never worked on Bank of England, Commercial, etc., systems, and she did not know what work was done by the Forschungsamt on these.

13. Interdepartmental Cypher.

(See Ticom/I-22, paragraphs 97 and 98)

HAGEN said that Pers ZS did not work on Interdepartmental Cypher, but only received results from OKW/Chi and the Forschungsamt. She believed that after the introduction of the new basic book in June, 1943, work on I.D. cypher was dropped and never started again. While it was being read, OKW, and RLM/FA interchanged results on I.D. Cypher and sent a copy to Pers ZS in 1940-41. There was no liaison with the services except possibly via the above organisations. She did not know anything about the work done by OKH on this system, but thought that they must certainly have had a copy of the captured book. OKW definitely did work on I.D. and probably was the first bureau to tackle it. She knew of no cryptanalytic exchange with Japan on this subject.

14. Liaison with other Bureaux

HAGEN stated that Pers ZS had no liaison with RLM/FA except on the subject of I.D. Cypher. They sent all their results to OKW/Chi but received little in exchange except groups from systems B 30 and 31. They gave OKW all the Irish substitution and subtractor keys. They also sent their results from B 30 and 31 to 4 SKL III but received nothing in return. No results were exchanged with OKH, Ob. d. L. or Wetterdienst. She only knew of work on British systems done by OKW and FA.

15. Organisation of Pers ZS.

HAGEN gave the following details of the organisation of the English group of Pers ZS at various times:-

1930. 5 or 6 people, including HOFFMANN and HAGEN. Changing.

1939. 5 or 6, including HOFFMANN, HAGEN, Frl. WERNICK and Frl. NOLL (for Spanish and Portuguese.)

1943. 8 or 10: WERNICK, NOLL - Assistant (Sachbearbeiter)
Frl. SEELE, Frau OFFERMANN - Assistant.
Frl. Dr. GALUSCHKA - scientific assistant (on Siamese and South America)
Frl. FELLBAUM, BUHLER, FINKEN and TITSCHACK - linguist clerks.

1945. 12 or 13 (including all the above except OFFERMANN and BUHLER)
Frl. VOSS, ROBCKE, KAUFF and Dr. FAHRENHOLZ - linguist clerks.

WERNICK, NOLL and GALUSCHKA were the cryptographers.

16. Chilean, Mexican and Argentine Systems.

(Pers ZS possessed photostat copies of the Chilean SOLAR Code and the Mexican XEPIT Code.) HAGEN said that the SOLAR Code consisted of alphabetical groups of 3 letters (indicating, inter alia, tenses) and 4 letters (always ending with Y or Z), each in alphabetical order. There were tables of 2 letter groups, giving frequent short words, articles and particles, and single-letter groups for the numbers and months. Clear words were indicated by the 2 letter group DY.

HAGEN was asked about the system by which blocks of groups in the XEPIT code-book are omitted. She replied that they had not discovered any systematic arrangement although they had done a lot of work on this problem. There were three similar books in succession, overlapping. The last of these was only partially alphabetical, i.e. the groups on the pages were alphabetical but the pages themselves were not in order. The book was sometimes used by substituting group 3, 5, 8 etc. below the actual group intended. The final group indicated how many groups away were to be substituted, special groups were used for this purpose but were identifiable from message to message.

17. HAGEN knew of three Argentinian systems:-

a) A 5-figure alphabetical code of 100,000 groups. This had an annex for geographical and proper names consisting of a few thousand groups. A fixed difference was generally used, e.g. for 119876 0123456, they would transmit 119976 123556. These differences were constant for each link but differed between links. Generally the difference was 50, 100 or 150.

b) A 5-figure alphabetical code of about 80,000 groups. It only went up to letter O groups inclusive. There was an annex for spellers, bigrams, trigrams and numbers.

c) In the last year or two they introduced a new 5-letter code which was similar to the others but the code words were restricted to groups beginning R,S,T and U - mostly T and U. They had little material on this code.

18. General.

HAGEN said that the most profitable British systems were the unreoyphered low grade codes, B 25 at the beginning of the war, and later B 31. She received her instructions direct from the Staats-sekretär. Although she worked almost exclusively on single-process British codes, this was not due to any lack of cryptographic ability. In fact this was probably the simplest side of her work and she took the lead in her section in breaking the Spanish, Portuguese and South American cyphers which presented very much stiffer cryptographic problems. She was not at any time a member of the Nazi party.

B. INTERROGATION OF O.R.R. ADOLF PASCHKE

1. Paschke worked as a cryptographer for the German Army 1915-1919. Joined Pers ZS 1919. Joined Nazi Party 1933. Home address - Berlin, Wilmersdorf, Johannisbergstrasse 17a.

2. SELCHOW (Director Pers ZS) as a rule dealt direct with RIBBENTROP and did not go through SCHRODER and/or WEIZSACKER.

3. The instructions from RIBBENTROP were invariably of a general nature and solely concerned with the subject matter of intelligence - e.g. Poland - or the invasion. He did not concern himself with the details of different systems in any way.

4. RIBBENTROP was well aware that the more important intelligence could only be gained from attacking the recyphered systems, but he was apparently satisfied not to press for the additional staff which would be required and contented himself with the material obtained from the single process codes.

4. RIBBENTROP was well aware that the more important intelligence could only be gained from attacking the recyphered systems, but he was apparently satisfied not to press for the additional staff which would be required and contented himself with the material obtained from the single process codes.

5. PASCHKE's view is that a depth of at least 6 was necessary to break a long subtractor on an unknown book and at least 3 on a known book.

6. Best depths on Foreign Office cyphers about 20. This was at the beginning of the war.

7. They worked on all traffic - Embassies, Legations and Consulates.

8. He thinks the O.K.M. had the biggest staff - about 400. None of the other bureaux had more than 300.

9. RIBBENTROP only read about 20% or 30% of the material produced. His secretaries, e.g. Herr WEBER and Herr LOESCH selected these for him.

10. F.A. read I.D. for a short time in Summer 1941.

11. Ministerialrat FENNER (believed in Bavaria) (in 1944 M.R. WENDLAND assisted him) - held the same position in O.K.W. as PASCHKE in Pers ZS and was a good friend of his, both being born in St. Petersburg. His (FENNER'S) immediate chief was Oberst KETTLER and his (KETTLER'S) was General GIMMLER, then KEITEL.

12. In F.A. Ministerialdirigent SCHRODER held the corresponding position to PASCHKE. Ministerialdirektor SCHAPPER was above him and then GOERING.

13. The German secret cypher systems PASCHKE believed to be first class.

14. O.R.R. LANGLOTZ was head of department of Auswertiges Amt dealing with German cyphers.

15. In 1944 O.K.W. (FENNER) took over the organisation of O.K.M, O.K.L. and O.K.H. cypher construction.

16. PASCHKE considers that of the three high AA officials concerned with diplomatic traffic von RIBBENTROP took most interest as had von NEURATH before him. The most interested of all was von RATHENAU (1922).

17. The reading of code telegrams besides giving occasional 'highlights' provided a wealth of press material not otherwise available.

18. The Staatssekretär decided on the distribution of telegrams in the A.A.

19. All the Pers ZS papers (40 chests) believed to have gone south to Bavaria from Muhlhaus in mid-April 1945. There were no other copies left.

20. Individual texts bore no marking but the files and folders were marked Geheime Reichssache.

21. No attack was ever attempted on British Attaché Cyphers. They were considered O.K.W.'s "pigeon".

22. PASCHKE was in practice the "Cypher Security" Adviser for the A.A.

23. Frau PASCHKE worked in Dr. PASCHKE's section for three years, but only as a clerk. She has never been asked by the Russians (from whom she obtains permits to visit PASCHKE from Berlin to Marburg) what she did or what her husband's profession was. PASCHKE enquired as to the possibility of the British providing air transport for Frau PASCHKE to join him at Marburg.